

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S7	259	(diffie adj hellman) and (elliptic adj curve)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:17
S8	82	S7 and @ad<"19990709"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 09:46
S9	205	OBERTHUR.as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:06
S10	1686	knudsen.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:06
S11	48	(knudsen and erik).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:06
S12	4	S11 and \$crypt\$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:08
S13	30	S9 and \$crypt\$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:09
S14	0	S8 and (genus adj (two "2"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:14
S15	0	S8 and (genus)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:14
S16	2	"380".clas. and (genus adj (two "2"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:15
S17	5	S8 and (halv\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:15
S18	1	(diffie adj hellman) and (point adj (divi\$4 halving))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:17
S19	4	(elliptic adj curve) and (point adj (divi\$4 halving))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 07:20
S20	0	(point adj halving) and (genus)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:06

S21	ABS + Kwll	25	(point adj halving)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:06
S22		2	S21 and elliptic	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:06
S23		0	(non adj super adj singular)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:17
S24		185	schroeppel.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:17
S25	ABS + Kwll	5	S24 and \$crypt\$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:19
S26		1	("6490352").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	OFF	2005/01/25 08:42
S27		1	point adj fractioning	US-PGPUB; USPAT; EPO; JPO; IBM_TDB	OR	ON	2005/01/25 08:22
S28	ABS + Kwll	6	point adj fractioning	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 08:23
S29		1	("20020061104").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	OFF	2005/01/25 08:23
S30		1	("20020041681").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	OFF	2005/01/25 08:52
S31		1	("6141420").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; IBM_TDB	OR	OFF	2005/01/25 08:52
S32		0	@ad<"19990709" and (non adj super adj singular)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 09:46
S33	ABS + Kwll	1	@ad<"19990709" and (super adj singular)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 10:24
S34		0	"Efficient Arithmetic on Koblitz Curves"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 10:24
S35		646	schroeppel	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 11:26

S36	185	schroeppel.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 11:26
S37	5	schroeppel.in. and \$crypt\$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 11:26
S38	4	schroeppel.in. and elliptic	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 13:26
S39	27	supersingular	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 13:56
S40	0	(elliptic adj curve) adj (odd adj order)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 13:56
S41	0	(elliptic adj curve) adj (odd)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 13:57
S42	1	(elliptic adj curve) and (odd adj order)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:03
S45	1137	knudsen	EPO; DERWENT	OR	ON	2005/01/25 14:00
S46	2	knudsen and elliptic	EPO; DERWENT	OR	ON	2005/01/25 14:00
S47	20	(elliptic adj curve) and (odd with point)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:08
S50	1255	(de adj la adj rue).as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:09
S51	0	(de adj la adj rue).as. and elliptic	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:08
S53	0	(de adj la adj rue).as. and knudsen	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:09
S54	0	(de-la-rue).as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:09
S55	1255	("de la rue").as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:09
S56	1	("de la rue" adj card).as.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/01/25 14:09

09786756

Michael J. Simitoski

Michael.Simitoski@uspto.gov

(571) 272-3841

### **Google**

knudsen "point halving"

Elliptic Scalar Multiplication Using Point Halving

schroeppel "point halving"

odd order point supersingular elliptic halving

"elliptic curve" "odd order" "non-supersingular"

"elliptic curve" "non-supersingular" "characteristic two" halving

schroeppel halving

koblitz "odd order" point

### **ACM**

knudsen "point halving"

### **IEEE**

("elliptic curve" <or> "finite field") <and> "point halving"

### **Other**

Search tool

Search Terms

### **Applications/Patents from Inventor Search**

see 892